R E P U B L I Q U E  F R A N Ç A I S E

10/665 801

10.29

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION

## CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 05 SEP. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

# BREVET D'INVENTION
# CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

## REQUÊTE EN DÉLIVRANCE 1/2

Réservé à L'INPI

Cet imprimé est à remplir lisiblement à l'encre noire

REMISE DES PIÈCES
DATE 20 SEPT 2002
LIEU 38 INPI GRENOBLE
N° D'ENREGISTREMENT 0211671
NATIONAL ATTRIBUÉ PAR L'INPI
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 20 SEP. 2002

**Vos références pour ce dossier**
*(facultatif)* B5622

❶ NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

**Cabinet Michel de Beaumont**
**1 rue Champollion**
**38000 GRENOBLE**

**Confirmation d'un dépôt par télécopie** ☐ N° attribué par l'INPI à la télécopie

| ❷ NATURE DE LA DEMANDE | Cochez l'une des 4 cases suivantes | |
|---|---|---|
| Demande de Brevet | [X] | |
| Demande de certificat d'utilité | ☐ | |
| Demande divisionnaire | ☐ | |
| *Demande de brevet initiale* | N° | Date / / |
| *ou demande de certificat d'utilité initiale* | N° | Date / / |
| Transformation d'une demande de brevet européen *Demande de brevet intiale* | ☐ N° | Date / / |

❸ TITRE DE L'INVENTION (200 caractères ou espaces maximum)

MASQUAGE DE DONNÉES DÉCOMPOSÉES DANS UN SYSTÈME DE RÉSIDUS

| ❹ DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE | |
|---|---|
| | Pays ou organisation |
| | Date N° |
| | Pays ou organisation |
| | Date / / N° |
| | Pays ou organisation |
| | Date / / N° |
| | ☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé "Suite"** |

| ❺ DEMANDEUR | | |
|---|---|---|
| | | ☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé "Suite"** |
| Nom ou dénomination sociale | | STMicroelectronics SA |
| Prénoms | | |
| Forme juridique | | Société anonyme |
| N° SIREN | | |
| Code APE-NAF | | |
| ADRESSE | Rue | 29, Boulevard Romain Rolland |
| | Code postal et ville | 92120 MONTROUGE |
| Pays | | FRANCE |
| Nationalité | | Française |
| N° de téléphone *(facultatif)* | | |
| N° de télécopie *(facultatif)* | | |
| Adresse électronique *(facultatif)* | | |

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

**BREVET D'INVENTION**
**CERTIFICAT D'UTILITÉ**
Code de la propriété intellectuelle-Livre VI

**REQUÊTE EN DÉLIVRANCE 2/2**

Réservé à L'INPI

REMISE DES PIÈCES
DATE 20 SEPT 2002
LIEU 38 INPI GRENOBLE
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0211671

| | | |
|---|---|---|
| **Vos références pour ce dossier :** *(facultatif)* B5622 | | |
| **⑥ MANDATAIRE** | | |
| Nom | | |
| Prénom | | |
| Cabinet ou Société | | Cabinet Michel de Beaumont |
| N° de pouvoir permanent et/ou de lien contractuel | | |
| ADRESSE | Rue | 1 Rue Champollion |
| | Code postal et ville | 38000 GRENOBLE |
| N° de téléphone *(facultatif)* | | 04.76.51.84.51 |
| N° de télécopie *(facultatif)* | | 04.76.44.62.54 |
| Adresse électronique *(facultatif)* | | cab.beaumont@wanadoo.fr |
| **⑦ INVENTEUR (S)** | | |
| Les inventeurs sont les demandeurs | | ☐ Oui<br>☒ Non **Dans ce cas fournir une désignation d'inventeur (s) séparée** |
| **⑧ RAPPORT DE RECHERCHE** | | **Uniquement pour une demande de brevet (y compris division et transformation)** |
| Établissement immédiat ou établissement différé | | ☒ / ☐ |
| Paiement échelonné de la redevance | | **Paiement en trois versements, uniquement pour les personnes physiques**<br>☐ Oui<br>☒ Non |
| **⑨ RÉDUCTION DU TAUX DES REDEVANCES** | | **Uniquement pour les personnes physiques**<br>☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)*<br>☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* : |
| **Si vous avez utilisé l'imprimé "Suite", indiquez le nombre de pages jointes** | | |

**⑩ SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)**

**Michel de Beaumont**
**Mandataire n° 92-1016**

VISA DE LA PREFECTURE OU DE L'INPI

DUBLOR

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

# MASQUAGE DE DONNÉES DÉCOMPOSÉES DANS UN SYSTÈME DE RÉSIDUS

La présente invention concerne les traitements algorithmiques effectués sur des données numériques manipulées par un microprocesseur ou un circuit intégré. L'invention concerne plus particulièrement les traitements opérés sur des données numériques dans des applications cryptographiques de chiffrement ou d'authentification mettant en oeuvre des algorithmes dits sécurisés. Dans de telles applications, les données manipulées par les algorithmes et sur lesquels sont effectuées des opérations de base (additions, multiplications) doivent pouvoir être protégées contre le piratage, c'est-à-dire des attaques extérieures visant à découvrir des données secrètes et/ou l'algorithme de calcul.

Par exemple, lorsqu'un circuit intégré (qu'il s'agisse d'un microprocesseur ou d'un opérateur en logique câblée) exécute un calcul sur des données, ce calcul influe sur sa consommation. Une analyse de la consommation du circuit intégré pendant l'exécution de l'algorithme peut permette à un pirate de découvrir les données traitées ou l'algorithme qui les exécute. De telles attaques par analyse de la consommation d'un circuit intégré manipulant des données sont connues sous les dénominations SPA (Single Power Analysis) ou DPA (Differential Power Analysis).

Un exemple d'application de la présente invention concerne les procédures d'authentification de fichiers numériques (par exemple, audio) ou d'éléments de traitement électroniques (par exemple, cartes à puces) afin de valider l'autorisation de l'utilisateur à accéder à des informations (par exemple, données audio ou données sur la puce).

Pour des questions de rapidité de calcul et de facilité d'implémentation des algorithmes, les nombres sur lesquels on souhaite effectuer des opérations par des moyens de calculs automatiques peuvent être décomposés par application du théorème dit des restes chinois (CRT).

Le théorème des restes chinois, appliqué à des nombres entiers, peut s'exprimer de la façon suivante. Pour toute suite de nombres $m_i$ (i compris entre 1 et n) premiers entre eux et pour toute suite d'entiers $x_i$, il existe un unique nombre entier x inférieur au produit de la suite de nombres premiers de la base de décomposition, tel que pour tout i:

$x_i$ = x modulo $m_i$.

Cela signifie que, pour une suite finie de nombres $m_i$, premiers entre eux, on peut représenter tout nombre inférieur au produit de cette suite finie de manière unique, en une suite d'entiers positifs en nombre égal au nombre d'éléments de la suite de nombres premiers entre eux. Cette représentation est appelée la représentation par système de résidus (Residu Number System, RNS).

En d'autres termes, pour tout nombre entier x compris entre 0 et M, où M représente le produit des nombres premiers entre eux $m_i$ de la base de décomposition, on peut écrire :

$$x = \left| \sum_{i=1}^{n} x_i \cdot m_i \cdot \left| M_i^{-1} \right|_{m_i} \right|_M , \qquad \text{(formule 1)}$$

avec $M = \prod_{i=1}^{n} m_i$, $M_i = \frac{M}{m_i}$, et où $\left| M_i^{-1} \right|_{m_i}$ est l'inverse du nombre $M_i$ modulo $m_i$. La notation $|\cdot\cdot|_M$ est utilisée pour désigner un nombre (ici, le résultat de la somme) modulo M.

L'intérêt des systèmes de résidus est que les opérations telles que l'addition, la soustraction et la multiplication sont simplifiées et peuvent être exécutées dans des architectures parallèles. En fait, les opérations élémentaires peuvent être effectuées sur chaque entier de la décomposition du nombre à calculer. Le résultat est ensuite obtenu en appliquant la formule 1 ci-dessus au résultat.

Par exemple, deux nombres x et y sur lesquels on souhaite effectuer un calcul sont décomposés en utilisant la même base de nombres premiers entre eux. Par suite, les opérations d'addition, de soustraction et de produit sont effectuées sur les éléments de la décomposition, modulo les nombres premiers correspondants. On obtient un ensemble de valeurs dans la base de décomposition, que l'on recombine pour obtenir le résultat.

L'intérêt majeur dans une exécution automatique des calculs au moyen de circuits intégrés est que les opérations individuelles modulo les nombres de la base de décomposition concernent des nombres ayant toujours la même taille, ce qui permet l'exécution de ces calculs au moyen d'architectures parallèles et dans une même durée.

Toutefois, un inconvénient est que les nombres traités sont plus facilement détectables par les différentes attaques, notamment, par analyse de la consommation du circuit intégré.

Classiquement, pour masquer le traitement d'un ou plusieurs nombres, on combine ces nombres avec des quantités aléatoires, avant le traitement algorithmique.

Un inconvénient est que cela modifie le ou les nombres traités, ce qui impose d'effectuer une modification inverse en fin de traitement pour récupérer le résultat attendu.

Un autre inconvénient est que le masquage accroît la complexité du traitement ainsi que la durée du calcul entier.

Plus généralement, le système des résidus appliquant le théorème des restes chinois s'applique lorsque les opérations et les opérandes sont celles d'un corps fini quelconque. Par

exemple, ce système s'applique à un corps de polynômes modulo un polynôme irréductible, ou au corps des entiers modulo un nombre premier.

La présente invention vise à proposer une solution pour masquer l'exécution de calculs algorithmiques utilisant des représentations par système de résidus.

L'invention vise plus particulièrement à proposer une solution de masquage qui soit indépendante de l'algorithme mis en oeuvre, c'est-à-dire qui puisse s'appliquer quels que soient les calculs exécutés sur les nombres décomposés.

L'invention vise également à proposer une solution qui ne nuit pas à la rapidité d'exécution de l'algorithme et, notamment, qui n'ajoute pas d'étape de calcul supplémentaire.

Pour atteindre ces objets et d'autres, la présente invention prévoit un procédé de masquage de données numériques manipulées par un algorithme et décomposées par un système de résidus à partir d'une base finie de nombres ou de polynômes premiers entre eux, consistant à rendre variable la base de décomposition.

Selon un mode de mise en oeuvre de la présente invention, la base de décomposition est choisie dans une table mémorisée d'ensembles de nombres ou de polynômes premiers entre eux.

Selon un mode de mise en oeuvre de la présente invention, l'ensemble de nombres ou de polynômes premiers entre eux, servant à la décomposition par système de résidus, est choisi aléatoirement dans la table mémorisée, à chaque nouvelle application de l'algorithme.

Selon un mode de mise en oeuvre de la présente invention, la base de décomposition est calculée par un générateur pseudo-aléatoire.

Selon un mode de mise en oeuvre de la présente invention, la base est choisie pour être compatible avec les longueurs des nombres ou polynômes traités par l'algorithme.

Selon un mode de mise en oeuvre de la présente invention, le procédé est appliqué à des données d'entrée déjà décomposées par un système de résidus dans une base d'origine, les données d'entrées subissant un changement de base de décomposition et le résultat fourni par l'algorithme subissant, de préférence, une transformation inverse vers ladite base d'origine.

Selon un mode de mise en oeuvre de la présente invention, le procédé est appliqué à des données d'entrée non encore décomposées.

Selon un mode de mise en oeuvre de la présente invention, un ou plusieurs changements de base de décomposition sont effectués pendant l'exécution de l'algorithme.

L'invention prévoit également un circuit de traitement algorithmique de données décomposées par un système de résidus à partir d'une base finie de nombres ou de polynômes premiers entre eux, comportant un circuit de sélection ou de génération, et de mémorisation temporaire de ladite base.

Selon un mode de réalisation de la présente invention, le circuit comporte un élément de stockage d'une table de bases de nombres ou de polynômes premiers entre eux, ledit circuit de sélection choisissant, à chaque application de l'algorithme, une base dans ladite table.

Selon un mode de réalisation de la présente invention, le circuit comporte un élément de vérification de conformité, entre la base sélectionnée pour application des décompositions par système de résidus et les circuits de calculs du circuit exécutant l'algorithme.

Ces objets, caractéristiques et avantages, ainsi que d'autres de la présente invention seront exposés en détail dans la description suivante de modes de réalisation particuliers faite à titre non-limitatif dans la figure annexée qui illustre, sous forme de blocs et de façon très schématique, un mode de mise en oeuvre du procédé de masquage selon l'invention.

Par souci de clarté, l'invention sera exposée ci-après en relation avec une application à des nombres entiers décomposés à partir d'une base de nombre premiers entre eux. On notera toutefois qu'elle s'applique plus généralement à une décomposition de polynômes d'un corps modulo un polynôme irréductible à partir d'une base de polynômes premiers entre eux.

Une caractéristique de la présente invention est de modifier la base de décomposition/recombinaison des nombres entiers traités par un algorithme en application d'un système de résidus.

Selon l'invention, on change la représentation par le système de résidus, de préférence, à chaque fois qu'un nouveau groupe de nombres entiers est soumis à une décomposition pour un traitement algorithmique, ou pour une opération de calcul.

Ainsi, à la différence des solutions classiques de masquage de calcul par l'introduction de nombres aléatoires dans les nombres traités pour modifier ceux-ci, l'invention prévoit de rendre variable la représentation du nombre, celui-ci restant inchangé.

Un avantage important par rapport à l'introduction d'un nombre aléatoire est que la récupération du résultat attendu ne nécessite pas de calcul supplémentaire par rapport à l'application classique des représentations par système de résidus. En effet, seule la base de décomposition doit être indiquée au processus de recombinaison classique. En d'autres termes, on rend la base de décomposition variable.

Un autre avantage est que la durée de calcul n'est que peu augmentée par le masquage. La seule durée supplémentaire correspond au changement de la base de décomposition (lecture en mémoire), ce qui est négligeable par rapport aux calculs supplémentaires requis, au moins en début et en fin d'algorithme, pour combiner les nombres (ou les polynômes) traités avec un nombre aléatoire.

La figure annexée représente, sous forme de blocs, un exemple d'application d'une représentation par système de résidus à un algorithme 1 (ALGO) devant traiter, par exemple, au moins deux nombres entiers x et y et fournir au moins un résultat r.

Comme précédemment, pour faciliter les calculs, l'algorithme 1 exécute des opérations élémentaires sur chaque élément de décompositions $\{x_1, \ldots, x_i, \ldots, x_n\}$, $\{y_1, \ldots, y_i, \ldots, y_n\}$ des nombres x et y dans la base de décomposition par un système de résidus. Cette décomposition s'effectue (blocs 2 et 3, BT) avant l'introduction des nombres dans l'algorithme 1 proprement dit, à partir d'une base $\{m_1, \ldots, m_i, \ldots, m_n\}$ de nombres premiers entre eux, où n représente le nombre d'éléments de la base qui correspond au nombre d'éléments des suites de décomposition des nombres x et y.

L'algorithme 1, c'est-à-dire le bloc de traitement, fournit le résultat sous la forme d'une suite de nombres entiers $\{r_1, \ldots, r_i, \ldots, r_n\}$. Cette suite de n nombres est, dans cet exemple, recombinée (bloc 4, IBT) à partir de la même base $\{m_1, \ldots, m_i, \ldots, m_n\}$ de nombres premiers pour obtenir le résultat r.

Selon la présente invention, la base de décomposition $\{m_1, \ldots, m_i, \ldots, m_n\}$ est fournie par un élément 5 (SELECT{M}) de sélection et de mémorisation temporaire de la suite de nombres (ou de polynômes) premiers entre eux de décomposition par système de résidus. Cette sélection est, de préférence, changée à chaque application de l'algorithme 1, c'est-à-dire à chaque nouvelle introduction de grandeurs x, y (à chaque fois qu'il est nécessaire de décomposer des valeurs à prendre en compte par le calcul algorithmique pour l'obtention d'un résultat recomposé sur la base du même système de résidus). Si plus de deux nombres sont utilisés, ou si d'autres nombres interviennent à d'autres moments dans l'algorithme, on veillera à maintenir une même base pour tous les nombres.

Selon la provenance et la destination des données d'entrée de l'algorithme, les décompositions 2 et 3 peuvent être faites plus en amont, par exemple, si les données d'entrées proviennent de sorties d'un traitement par système de résidus. De même, le ou les résultats peuvent être fournis sous forme décomposée. Cela sera notamment le cas si l'algorithme dont l'exécution est masquée par l'invention est imbriqué dans une chaîne de traitement utilisant un système de résidus. Dans ce cas, les blocs 2, 3 et 4 exécutent des changements de base pour convertir les données d'entrée représentées dans une certaine base de décomposition en une base sélectionnée par l'élément 5 et pour restituer les données de sorties dans la base d'entrée.

Selon un autre mode de réalisation, des changements de base (additionnels ou non) peuvent intervenir en cours de l'algorithme. Ces changements sont alors sélectionnés au moyen de bloc 5 de la même façon que la transformation initiale. La restitution des nombres traités est alors obtenue par une seule transformation inverse effectuée (pas nécessairement en fin d'algorithme) selon la dernière base utilisée.

Plusieurs méthodes peuvent être utilisées pour sélectionner la base de décomposition ou pour changer de base en cours de calcul.

Selon un premier mode de mise en oeuvre, une table 6 d'ensembles {M} de nombres premiers entre eux est stockée dans un élément de mémorisation et on prévoit une sélection (par exemple, aléatoire) d'un des ensembles de la table mémorisée à chaque nouvelle décomposition, chaque ensemble représentant une base dans le système des résidus.

Selon un autre exemple de mise en oeuvre, on utilise un générateur de suites de nombres premiers entre eux qui génère (à la volée), de façon pseudo-aléatoire pour être compatible avec l'architecture parallèle du circuit exécutant l'algorithme 1, la base de décomposition $\{m_1, \ldots, m_i, \ldots, m_n\}$.

On notera que, pour que la décomposition ou le changement de base soit différent d'un calcul à un autre, il

suffit que deux nombres de la base de décomposition choisie soient inversés, c'est-à-dire placés dans un ordre différent dans la suite des nombres de la base. Il est par conséquent particulièrement simple, de faire varier la décomposition de n'importe quelle donnée numérique d'entrée tout en restant compatible avec un même circuit de traitement par architecture parallèle. Il suffit de modifier l'aiguillage des données décomposées en fonction de l'ordre des nombres (ou des polynômes) premiers entre eux de la base. Le mode de transformation de la base par changement d'ordre des nombres de celle-ci conditionne cependant la qualité du caractère aléatoire de la représentation des nombres dans le système des résidus.

Un avantage de la présente invention est que sa mise en oeuvre est indépendante de l'algorithme exécuté.

Un autre avantage de l'invention est qu'elle ne nécessite pas de recalcul spécifique à l'issu de l'algorithme pour récupérer le nombre attendu. En effet, dans toute structure à traitement algorithmique par application du théorème des restes chinois, une étape de recombinaison à partir de la base de nombres ou polynômes premiers entre eux est prévue pour restituer le résultat.

Un exemple d'algorithme où l'invention s'applique est l'algorithme de type RSA tel que décrit dans l'article "Modular multiplication and base extension in residue number systems" de J.-C. Bajard, L.-S. Didier et P. Kornerup, publié par N. Burgess, rapport de Arith 15, 15ème symposium IEEE sur l'arithmétique informatique, Vail, Colorado, USA, Juin 2001, pages 59-65.

Bien entendu, la présente invention est susceptible de diverses variantes et modifications qui apparaîtront à l'homme de l'art. En particulier, l'invention s'applique quel que soit le nombre de données d'entrée de l'algorithme et quel que soit le nombre de données fournies par cet algorithme, pourvu que toutes les données d'entrée soient décomposées à partir de la même base de nombres ou polynômes premiers entre eux.

De plus, le choix de la taille des ensembles de nombres ou polynômes premiers constituant la base de décomposition dépend de l'application et est choisi de façon classique.

En outre, la réalisation pratique de l'invention à partir des indications fonctionnelles données ci-dessus est à la portée de l'homme du métier en utilisant des moyens connus. La mise en oeuvre de l'invention peut être logicielle ou par des machines d'états en logique câblée. Par exemple, mis en oeuvre de façon matérielle, les blocs 2 et 3 de décomposition ou de changement de base des données d'entrée peuvent être constitués d'un ou plusieurs circuits selon que le changement de base est effectué en parallèle ou successivement pour les différentes données d'entrée.

## REVENDICATIONS

1. Procédé de masquage de données numériques manipulées par un algorithme (1) et décomposées par un système de résidus à partir d'une base finie de nombres ou de polynômes premiers entre eux, caractérisé en ce qu'il consiste à rendre variable la base de décomposition.

2. Procédé selon la revendication 1, caractérisé en ce que la base de décomposition est choisie dans une table mémorisée (6) d'ensembles de nombres ou de polynômes premiers entre eux.

3. Procédé selon la revendication 2, caractérisé en ce que l'ensemble de nombres ou de polynômes premiers entre eux, servant à la décomposition par système de résidus, est choisi aléatoirement dans la table mémorisée (6), à chaque nouvelle application de l'algorithme (1).

4. Procédé selon la revendication 1, caractérisé en ce que la base de décomposition est calculée par un générateur pseudo-aléatoire.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que la base est choisie pour être compatible avec les longueurs des nombres ou polynômes traités par l'algorithme.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il est appliqué à des données d'entrée déjà décomposées par un système de résidus dans une base d'origine, les données d'entrées subissant un changement (2, 3) de base de décomposition et le résultat fourni par l'algorithme (1) subissant, de préférence, une transformation inverse (4) vers ladite base d'origine.

7. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il est appliqué à des données d'entrée non encore décomposées.

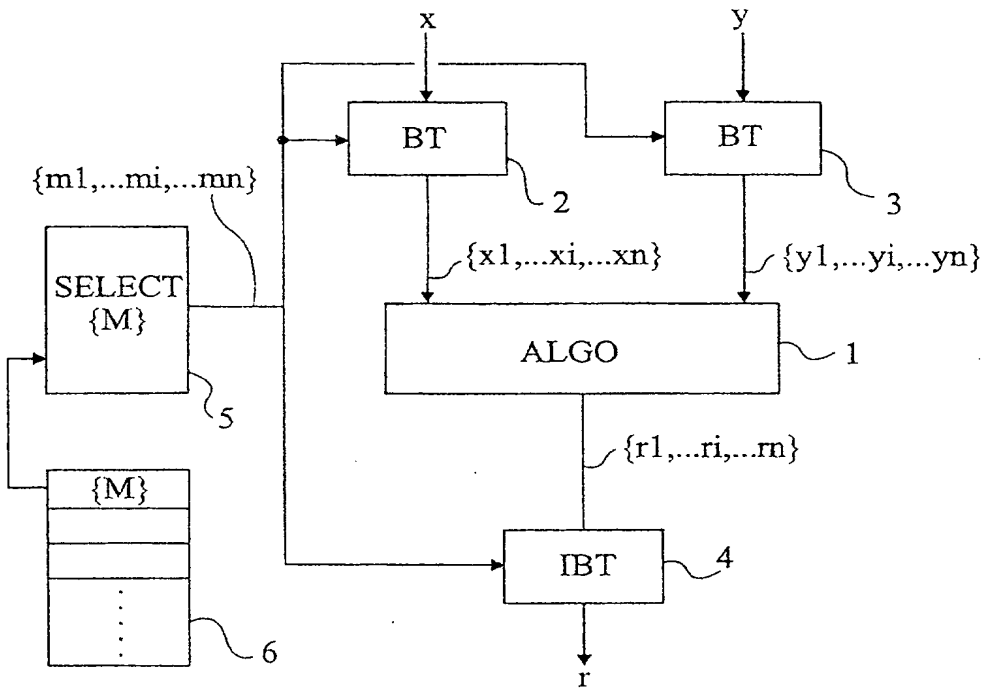
8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'un ou plusieurs changements de base de

décomposition sont effectués pendant l'exécution de l'algorithme (1).

9. Circuit de traitement algorithmique de données décomposées par un système de résidus à partir d'une base finie de nombres ou de polynômes premiers entre eux, caractérisé en ce qu'il comporte un circuit (5) de sélection ou de génération, et de mémorisation temporaire de ladite base.

10. Circuit selon la revendication 9, caractérisé en ce qu'il comporte un élément (6) de stockage d'une table de bases de nombres ou de polynômes premiers entre eux, ledit circuit de sélection (5) choisissant, à chaque application de l'algorithme, une base dans ladite table.

11. Circuit selon la revendication 9 ou 10, caractérisé en ce qu'il comporte un élément de vérification de conformité, entre la base sélectionnée pour application des décompositions par système de résidus et les circuits (1) de calculs du circuit exécutant l'algorithme.


x
y
BT
BT
2
3
{m1,...mi,...mn}
{x1,...xi,...xn}
{y1,...yi,...yn}
SELECT
{M}
ALGO
1
5
{r1,...ri,...rn}
{M}
IBT
4
6
r

Fig

reçue le 09/10/02

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

cerfa N° 55 -1328

# BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

## DÉSIGNATION D'INVENTEUR(S) PAGE N°1/ 1

**(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)**

Cet imprimé est à remplir lisiblement à l'encre noire

| | |
|---|---|
| **Vos références pour ce dossier** *(facultatif)* | B5622 |
| **N° D'ENREGISTREMENT NATIONAL** | 02 11671. |

**TITRE DE L'INVENTION** (200 caractères ou espaces maximum)

MASQUAGE DE DONNÉES DÉCOMPOSÉES DANS UN SYSTÈME DE RÉSIDUS

**LE(S) DEMANDEUR(S) :**

STMicroelectronics SA

**DESIGNE (NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite "Page N°1/1" S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).**

| | | |
|---|---|---|
| Prénoms & Nom | | Pierre-Yvan Liardet |
| ADRESSE | Rue | 56, Rue du Pralou, Lotissement L'Audiguier |
| | Code postal et ville | 13790 PEYNIER, FRANCE |
| Société d'appartenance *(facultatif)* | | |
| Prénoms & Nom | | |
| ADRESSE | Rue | |
| | Code postal et ville | |
| Société d'appartenance *(facultatif)* | | |
| Prénoms & Nom | | |
| ADRESSE | Rue | |
| | Code postal et ville | |
| Société d'appartenance (facultatif) | | |

**DATE ET SIGNATURE (S)**
**DU (DES) DEMANDEUR(S)**
**OU DU MANDATAIRE**
**(Nom et qualité du signataire)**

**Michel de Beaumont**
**Mandataire n° 92-1016**

Le 20 septembre 2002

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.